Modeling and Verification of Insider Threats Using Logical Analysis

Florian Kammüller*, Christian W. Probst§
§Technical University of Denmark
cwpr@dtu.dk
*Middlesex University London, UK
f.kammueller@mdx.ac.uk

***Abstract*—In this paper we combine formal modeling and analysis of infrastructures of organisations with sociological explanation to provide a framework for insider threat analysis. We use the Higher Order Logic proof assistant Isabelle/HOL to support this framework. In the formal model, we exhibit and use a common trick from the formal verification of security protocols showing that it is applicable to insider threats. We introduce briefly a three step process of social explanation illustrating that it can be applied fruitfully to the characterisation of insider threats. We introduce the Insider theory constructed in Isabelle that implements this process of social explanation. To validate that the social explanation is generally useful for the analysis of insider threats and to demonstrate our framework, we model and verify the insider threat patterns Entitled Independent and Ambitious Leader in our Isabelle/HOL framework.**

***Index Terms*—Insider threats, formal modeling, automated verification**

I. Introduction

In this paper, we show that formal modeling techniques and logic can be applied to model and analyse insider threats. The main target of the verification is to scrutinize abstract models of cyber-humane systems, i.e., systems that integrate organisations, policies, and actors. We ground our methodology on two pillars: the process of sociological explanation originating in the work of the sociologist Max Weber [1], and formal methods from computer science. For the practical support, we use verification tools common in safety assurance of technical systems or security proofs of authentication protocols. Drawing from the experience with the latter application, we show that the classical attack on the Needham-Schroeder asymmetric authentication protocol can be seen as an early insider attack [2]. The central part for the analysis of this protocol shows that insider threats are linked with personality splits of actors. This decisive cue can be extracted and applied to insider threat analysis within Weber's social explanation. Max Weber uses three steps from the macro-level to the micro-level and back to explain sociological phenomena. Following this process of social explanation, we provide a model integrating the context of an organisation with actors, the policies that apply to actors and locations and the psychological disposition of the actors. We illustrate that the three steps of sociological explanation can be applied to insider threat cases using Isabelle/HOL [3]. This interactive theorem prover has been successfully applied to security protocol analysis. We use it to provide a mechanized logical framework for insider threat analysis and illustrate its use on two patterns of insider attacks: the Entitled Independent and the Ambitious Leader [4]. In comparison to earlier work on insider threat analysis with modelcheckers [2], [5], the current approach allows the integration of macro and micro-level views in one complex model: the views of an organisation as a graph of locations and actors where policies are locally attached but also globally evaluated and where actors have psychological dispositions. It is the expressiveness of Higher Order Logic in Isabelle/HOL that enables such complex models and proofs of security properties. The framework we provide as an extension of the generic interactive theorem prover Isabelle/HOL provides a tool to analyse insider threats on infrastructure models including humans using social explanation. In practice, such a tool can be used to model and analyse infrastructures of organisation and their policies to detect vulnerabilities to insider attacks in order to provide new security architectures or to improve existing ones.

A. Overview

In Section II, we present the first insider as the intruder of the Needham-Schroeder attack elaborating that it is the switch of the intruder's personality that enables the attack. We next present a brief summary of social explanation following Max Weber (Section III) illustrating its application to model insider threats on the Dropbox example. The example has been used in various works [6] including our own [2], [7]. Here we aim at generalizing the observation that Weber's three steps are a good model for insider threats. Drawing from the CERT Guide to Insider Threats [4], we briefly introduce the patterns of Insider Threats as identified by the CERT Insider Threat Center at CMU: *theft, sabotage, and fraud*. In this paper we focus on *theft* picking the two general patterns of insider attacks on intellectual property defined as the major insider patterns for theft [4]: the Entitled Independent and the Ambitious Leader. We extend here the Isabelle/HOL model for social explanation of insider threats [7] to a more general framework and illustrate it on these general insider patterns in Section IV validating the application by properties of insider threats that can now readily be proved in Isabelle/HOL in our model. The personality split discovered in the Needham Schroeder protocol provides the means to formally prove that the CERT attacks are possible in vulnerable infrastructures.

II. The First Insider: Needham-Schroeder's Intruder

The attack on the Needham-Schroeder Public Key protocol has often been used as an example to show the superiority of formal techniques over good engineering practice. The attack is a result of a change of security assumptions about the communication context. Needham and Schroeder designed this protocol as one of the first cryptographic protocols a few years after the invention of public key cryptography. This was the time when the first email systems were installed, and the Internet was still in its infancy. It was safe to assume that the principals that participated in network communication protocols were part of some group of honest people who did not act as attackers simultaneously. Therefore, it is understandable that even in 1990 when the BAN logic [8] was conceived and logical analysis was for the first time applied to security protocols, the flaw in the Needham-Schroeder Public Key protocol (NSPK) still was not discovered. It was only five years later, in a world that already saw the advent of the Internet as a public and anonymous communication space, that Lowe identified a seemingly obvious but crucial attack on NSPK. The attack does not need to break any cryptography and still allows the attacker to impersonate a member of the network. This attack is at the same time the first *insider* attack since it is based on the fact that a seemingly trustworthy participant of the group of principals acts simultaneously as attacker. To the best of our knowledge, this basic fact about the attack has been overlooked till now. Usually the attack is characterized as a classical man-in-the-middle attack – which is only half-true. We first briefly recapitulate the NSPK protocol and its attack to show that it is an insider attack. Moreover, we use the attack to illustrate that a refinement on the data can be used to make the attack discoverable and that this remedy also secures the protocol.

We use the short form of the Needham Schroeder Public Key Protocol (NSPK) originally published by [9]. The protocol is usually written as follows using public keys K_A, K_B known globally and their secret counterparts K_A^{-1}, K_B^{-1} establishing nonces N_A, N_B in the process of authentication.

$$\begin{array}{lcl} A \to B & : & \{N_A, A\}_{K_B} \\ B \to A & : & \{N_A, N_B\}_{K_A} \\ A \to B & : & \{N_B\}_{K_B} \end{array}$$

The originally published protocol gives rise to the well-known attack of [10].

The attack goes as follows. The insider I is a normal member of the network. Therefore, he has like any A and B also an address and his public key K_I – for which only he has the corresponding private key K_I^{-1} – is known in the communication network. What is more is that I is a peer, i.e., principals do actually communicate with I. This fact is the main clue for the attack and also the reason why this is an insider attack. I must wait for A to request a communication with I, i.e., A sends a message according to step one of the protocol to I. Now, I sets up a parallel session, pretends to be A towards B initiating a second "Step One" this time from $I(A)$ to B, i.e., from I using B's sender address. We show the attack next using these notations but numbering the protocol steps according as $\alpha.i$ and $\beta.i$ for $i \in \{1..3\}$ for each of the parallel sessions.

$$\begin{array}{lcll} \alpha.1 & A \to I & : & \{N_A, A\}_{K_I} \\ \beta.1 & I(A) \to B & : & \{N_A, A\}_{K_B} \\ \beta.2 & B \to I(A) & : & \{N_A, N_B\}_{K_A} \\ \alpha.2 & I \to A & : & \{N_A, N_B\}_{K_A} \\ \alpha.3 & A \to I & : & \{N_B\}_{K_I} \\ \beta.3 & I(A) \to B & : & \{N_B\}_{K_B} \end{array}$$

Looking at the steps, we can see that I switches between the roles of I and $I(A)$ at his leisure. The attack appears to be some kind of man-in-the-middle attack but it is really only successful as such towards B. While A quite rightly believes that he speaks with I – as he intended to – B believes he speaks to A while he really speaks with I.[1] The NSPK attack is easily fixed by introducing the sender B in step 2.

$$\begin{array}{lcl} A \to B & : & \{N_A, A\}_{K_B} \\ B \to A & : & \{N_A, N_B, B\}_{K_A} \\ A \to B & : & \{N_B\}_{K_B} \end{array}$$

This fix of the attack has been also discovered by Lowe who found the attack in the first place a year later using modelchecking with CSP/FDR [11].

As discussed, the attack is an insider attack since it only works if A addresses I as a legal member of the network. The switch between the two roles I and $I(A)$ could be considered as acting schizophrenically if it would not be intentional directed to the purpose of impersonation. The fact that this switch is possible is another necessary and sufficient condition for the success. Translated into practical terms, the notion of $I(A)$ could be implemented by IP packets with a fake sender IP address (which is perfectly possible in the Internet protocol IP and is also known as *spoofing*).

It is this split of personality that makes the attacker an insider and simultaneously it is this split as well that enables the attack. Based on this observation, we construct a generic insiderness property called `UasI` in Section IV-D

III. Sociological Explanation: Max Weber's Three Steps

All sciences seek to find truth. The philosopher Popper describes that it is 'imperative to see and solve the most urgent problems and to solve them by creating true theories' [12]. Theories cannot correspond one-to-one to reality. They need to abstract from reality. Therefore, the creation of true theories according to Popper's words can only be an approximation of reality because any theory differs from the reality in which the phenomena it describes exist. But any useful theory should be consistent with the reality it describes and contain enough detail to explain the phenomena that we are interested in.

[1] Even though the attack seems only half way successful, it can be exploited. Assume B is a bank and I sends a message "transfer 1000 $ from my account to that of I" after the attack using A's credentials.

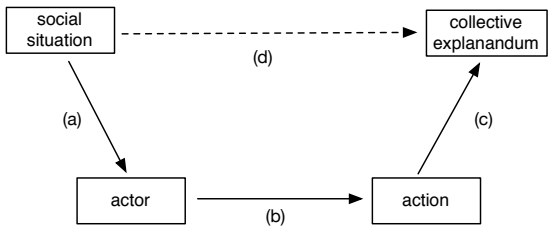

Fig. 1. The 'Grundmodell' of sociological explanation [15]

Tarski's conception of correspondence of theories explains exactly this [13], [14]. This conception laid the foundation to model theory for mathematical logic and is equally seen as philosophical foundation in sociology in the school of critical rationalism [15]).

Max Weber is one of the leading figures in the early development of sociology. According to him the basic process of sociology is 'understanding explanation' (*Verstehendes Erklären*) [16]. This process of sociological explanation has three steps: (a) the 'interpreting understanding' (*Deutendes Verstehen*), where the sociologists needs to understand how the actors interpret their situation, (b) the subjectively meaningful action of the actor, and (c) the effects of the action (see Figure 1).

The three steps of Max Weber have a level of interpretation that is not known in other sciences (Boudon [17]). Alfred Schütz has taken this observation further [18] by coining the notion of *constructions of first order* for the subjective ideas of the actors that determine step (a) of the sociological explanation while he described the models explaining the steps of action (b) and effects (c) as *second order constructions*. The aspect of interpretation of the process of sociological explanation seems to require unusual logics of explanation. Nevertheless, Weber, Boudon, as well as Schütz have emphasized that the subjectivity of the social has to be treated with the same objective methods of other sciences [15].

The explanation of sociological phenomena uses a three layered approach following the *logic of explanation* [19] that corresponds to Weber's three steps. This approach refines the three steps as described in Figure 1 by introducing a view on *actors*. The explicit modeling of humans as actors gives rise to distinguish a *macro*-level view from a *micro*-level view. The three steps of Weber's model together form a macro-micro-macro-transition explaining sociological phenomena by breaking down the global facts from the macro level (a) onto a more refined local view of individual actors at the micro-level (b). Finally those micro-steps are generalized and lifted back onto the macro-level (c) to explain the global phenomenon. The formal description of this procedure is described by three transitions between dedicated logics. In the first step, a *situational logic* maps the global context (environment) onto the actor ((a) from the macro to the micro).

The second step in the micro-level of the individual actor (b) is described by a so-called *logic of selection* describing how the actor selects his actions based on the situation (or his perception thereof). The *logic of selection* describes how the actor makes his choice. Examples could be straightforward normative action models in which the actor follows – like an automaton – given rules according to predetermined *norms* or more dynamic forms of action models including, for example, cognitive learning.

The third step called *aggregation logic* comprises the micro-sociological results and lifts them back onto the macro-level to finally explain the social phenomenon that results.

The logic of explanation has been created in 1948 later than Weber's original [1] but it is possible to reconstruct his original hypotheses using this logic. In his analysis of Weber's arguments McClelland [20] casually uses the macro-micro-macro transition, when he reconstructs Weber's explanation of the relationship between 'protestant ethic' and 'the spirit of capitalism'. Protestantism has lead to changes in familial socialization, a 'familial revolution' (macro to micro-level). The change of educational style employed by protestant parents (micro-level) has equipped their children with 'strong internalized achievement drives'. This has created the spirit of capitalism back on the collective, the macro-level, and has lead to the spread of a new type of actor, the entrepreneur.

A. Sociological Explanation of Insider Threats

In order to approach a tentative model of human behaviour in HOL, we concentrate on our motivating application area of insider threats. We illustrate how each of Weber's three steps can be supported.

As a running example, we consider first a more data-centric view of insider attacks. Glasser and Lindauer [6] consider the generation of insider threat data using a synthetic data generation framework. The input to the data generation process is largely autonomous and produces intelligent near realistic data. However, the kernel ingredient to this process are basic insider scenarios that are manually inserted. These insider scenarios are constructed using counter-intelligence expert knowledge.

We consider here an example from [6] that nicely shows all three steps of the sociological process of explanation and that thus suits us very well as a test case to elicit requirements to a HOL model for human insider behaviour.

B. Insider Example: Dropbox

'A member of a group decimated by layoffs suffers a drop in job satisfaction. Angry at the company, the employee uploads documents to Dropbox, planning to use them for personal gain.' The data generation process derives so-called 'observables' from this scenario. For the example, the observables are given in the following list [6].

- Data streams end for laid-off co-workers, and they disappear from the LDAP directory.
- As evidenced by logon and logoff times, subject becomes less punctual because of a drop in job satisfaction.
- HTTP logs show document uploads by subject to Dropbox.

When considering building a theory of human behaviour, we can use this attack case since it shows the three steps of Weber's process and can thus serve for requirements elicitation for a comprising HOL model [7]. The situational logic needs to be able to model the process of (a) 'A member of a group decimated by layoffs suffers a drop in job satisfaction.', the logic of selection then must embed (b) 'Angry at the company, the employee uploads documents to Dropbox, planning to . . . ', and the aggregation logic should express (c) 'use them for personal gain', i.e., effects on the society, for example, damage to the company (workers and clients of company) and wider economical effects.

The Dropbox example is a first illustration that social explanation is a good method to analyse insider attacks. In the following we aim at exploring whether this method is generally applicable to the analysis of insider threats. To this end, we look at more general patterns of insider threats derived from real insider attack cases [4] and simultaneously at formalizing the method of social explanation for the analysis of insider threats in Isabelle/HOL.

IV. A HOL Model for Social Explanation of Insider Threats

In this section, we first introduce the logical model of actors, organisations, and policies formalized in Isabelle/HOL. While doing so we refer to the three steps of Weber's social explanation motivating specific elements of the model. We first briefly introduce Higher Order Logic, the logic that is implemented in Isabelle/HOL introducing specific constructs later on the fly when they are used.

A. Isabelle/HOL

Isabelle/HOL is an interactive proof assistant based on Higher Order Logic (HOL). It enables specification of so-called object-logics for an application. Object-logics comprise new types, constants and definitions and reside in theory files, e.g., the file `Insider.thy` contains the object-logic we define for social explanation of insider threats below. We construct our theory as a conservative extension of HOL guaranteeing consistency. I.e., we do not introduce new axioms that could lead to inconsistencies. As a support for this conservative extension, new datatype and inductive definitions can be defined by the user but their defining rules are derived in the background by Isabelle. The introduction of a new datatype automatically creates distinctiveness properties for its constructors, a case analysis rule, and an induction principle thus providing proof machinery for the application of the derived theory. Isabelle/HOL also offers the concept of locales [21] which supports modular reasoning [22]. Locales enable local proof contexts in which syntactic abbreviations, arbitrary but fixed variables, and assumed properties can be combined and then invoked later in proofs.

The Isabelle/HOL model for social explanation of Insider threats is contained in the theory `Insider.thy`. This theory provides a framework for modeling and analysing insider threats. As application case studies, we validate this framework on two of the three main classes of insider threats [4]. The two case studies are contained in `EntitledIndependent.thy` and `AmbitiousLeader.thy`, respectively. These are available online [23]. In the following, we introduce these three theories in detail. A more detailed introduction into modeling in HOL and comparison to social explanation is contained in [7].

B. Modeling Individuals and their Disposition

The transition from the macro-level to the micro-level (step (a) in Figure 1) necessitates a macro-level view but it is also determined by the insider's mental characteristics, e.g., psychological state and motivation to express how the situation creates the individuals disposition and thus triggers actions at the micro level. We first introduce the parts of our Isabelle/HOL model for this situational logic introducing actors and their psychological characteristics before we show the model of the context, i.e., the network of actors and locations that constitutes the macro-level.

Actors are modeled as an abstract type that is created via a constructor function `Actor` from identities which are just a synonym for the base type `string`.

```
typedecl actor
type_synonym identity = string
consts Actor :: string ⇒ actor
```

A recent framework for characterising insider threats [24] offers a taxonomy of insider threats based on a thorough survey on results from counterproductive workplace behaviour, e.g., [25], [26] and case studies from the CMU-CERT Insider Threat Guide [4]. The classes identified in this taxonomy are the *Precipitating Event* or catalyst, the individual's *Personality Characteristics*, *Historical Behaviour*, *Psychological State*, *Attitude Towards Work*, *Skill Set*, *Opportunity*, and *Motivation to Attack*. We chose to use this taxonomy as it is based on a considerable range of empirical research results and includes those taxonomy parts of the CMU-CERT patterns that are relevant for our psychological description of the disposition of insiders.

It is simple to model a taxonomy in HOL since classes are similar to types. We use here the concept of a HOL datatype. As an example, consider the formal representation of *Psychological State* as a datatype.

```
datatype psy_states = happy | depressed | disgruntled
                    | angry | stressed
```

The element on the right hand side are the five injective constructors of the new datatype `psy_states`. They are simple constants, modeled as functions without arguments.

Another example is *Motivation*.

```
datatype motivations = financial | political | revenge
                     | fun | competitive_advantage
                     | power | peer_recognition
```

A practical issue is the integration of causalities, quantification or qualification into this basic model. For example, if an employee is disgruntled this might give rise to a motivation of revenge. In [24], these causalities are expressed by drawing

lines between boxes containing the classes of the taxonomy. These dependencies resemble the relation between variables in the System Dynamics model (for an example, see Section VI-B). Such lines express dependencies, like 'motivation for revenge may be caused by anger' but this is not a logical causality, i.e., anger ⇒ revenge – a logical causality expresses that anger necessarily implies revenge motivation which might not be the case for all actors.

Logical implication is thus not adequate for expressing dependencies between taxonomy classes. However, HOL offers other constructs like sets, functions and relations that extend the taxonomy classes with a finer grain for modeling dependencies. The values identified for the different classes of the insider threat taxonomy are distinct values by construction since we defined them as the fields of a datatype. However, they may occur in combination. This can be easily achieved by building sets of criteria, like the following function that uses the type constructors `set` to define a set of motivations.

```
motivation :: motivations set
```

This construct allows later to attach a range of motivating values to an actor and consequently to use standard HOL-set relations to compare these for qualitative statements, e.g., `motivation_alice` ⊆ `motivation_bob` to express that the motivation to become an insider is higher for Bob. This takes us one step further to a more qualitative model of the insider taxonomy for (non-exclusive) insider criteria like motivation. However, for the `psy_state` datatype, combinations of values, e.g., {`happy, depressed`} may be meaningless and individualized relations like subtyping or inequalities are more useful to introduce a more fine grained qualification and dependencies. In order to add some quantification to each of these factors, it is useful to explicitly model a quantity as part of the assigning function for the actors. The quantity could contain any metrics for a given insider characteristics, e.g., a real number denoting some measure for any of the actors motivational values.

```
quant_motivation :: actor ⇒(real × motivation)
```

The *Precipitating Event* or *Catalyst* has a separate role in the characteristics given in the taxonomy. It can be any event that has the potential to tip the insider over the edge into becoming a threat to their employer. It has been called the 'tipping point' in the literature and can be formalized as a predicate on actors. In order to carry over to the micro-level representation, it is advisable to contain with it the various characteristics about the actor in a combined state.

```
datatype actor_state = State "motivation" "psy_state"
```

Finally, the catalyst is encoded as a tipping point predicate that describes the motivation of an actor to become an insider.

```
definition tipping_point :: actor_state ⇒ bool
tipping_point a ≡ motivation a ≠ {}
                  ∧ happy ≠ psy_states a
```

C. Modeling the Macro-Level and Behaviour

At the macro-level, we are interested in modeling the actors including the insider within their context. Therefore, we adopt an approach of modeling the organisation with the actors as a network that can contain various layers of physical, administrative and logical views inspired by Probst and Hansen [27]. This approach originally uses the Klaim calculus to model an organisation and its actors as a graph of locations and actors. Figure 2 shows an example of a physical model and its representation in ExASyM [28] used as starting points in the TREsPASS project. This example describes a company where the Janitor can access the printer room becoming an insider by picking up confidential printouts. The organisation's infrastructure (Figure 2, left) including actors, networks, locations, and policies can be expressed as a graph in ExASyM (Figure 2, right). This contextual model is a graph containing actor identities, locations like rooms but also logical locations like servers as its nodes. In our Isabelle/HOL framework, we represent these graphs algebraically. Using a polymorphic type variable `'n` we define graphs over arbitrary nodes, i.e., a graph can contain any type of nodes. We further define a type `node` unifying identities and locations allowing us to model infrastructure using a `node graph` (see below).

```
datatype location = Location nat
datatype node = NA identity | NL location
datatype 'n graph = Graph ('n × 'n)set
```

In order to explore insider behaviour in organisational models (corresponding to step (b) in Figure 1), we use an abstract view that is inspired by previous work on policy formalisations and analysis [2], [5]. There, invalidation of policies reveals insider attack vectors by modelchecking system and workflow specifications.

In the current more refined Isabelle/HOL model we express policies over actions `get`, `move`, `eval`, and `put`.

```
datatype action = get | move | eval | put
```

We abstract here from concrete data – actions have no parameters. Policies describe prerequisites for actions to be granted to actors given by pairs of predicates (conditions) and sets of (enabled) actions.

```
type_synonym policy = ((actor ⇒ bool) × action set)
```

We integrate policies with a graph into the infrastructure providing an organisational model where policies reside at locations and actors are adorned with additional predicates to specify their 'credentials'.

```
datatype infrastructure = Infrastructure
"node graph" "location ⇒ policy set" "actor ⇒ bool"
```

These local policies serve to provide a specification of the 'normal' behaviour of actors but are also the starting point for possible attacks on the organisation's assets. The `enables` predicate specifies that an actor `a` can perform an action `a'`∈ `e` at location `l` in the infrastructure `I` if `a`'s credentials (stored in the tuple space `tspace I a`) imply the location policy's (stored in `delta I l`) condition `p` for `a`.

```
enables I l a a' ≡
 ∃ (p,e) ∈ delta I l. a' ∈ e ∧ (tspace I a ⟶ p(a))
```

The behaviour abstractly specifies that good actors respect the global policy.

```
behaviour I ≡ {(t,a,a'). enables I t a a'}
```

Attacks can be found efficiently by invalidating a global policy and then analysing whether the local policies enable the actors to achieve a state violating this policy. This analysis is the aggregation logic of the three steps of social explanation. It leads back to the macro level (step (c) in Figure 1) thus connecting macro and micro level to show how an insider attack can be performed.

D. Connecting Macro and Micro Level: Insiderness

Analysis of protocol verification, like the classical Needham-Schroeder public key attack and other insider threat case studies [2] show that a recurring scheme in insider attacks lies in role identification as described in Section II. We define this role identification by the `UasI` predicate. It expresses that the insider plays a loyal member of an organisation while he simultaneously acts as an outside attacker.

```
UasI a b ≡ (Actor a = Actor b)
```

Insider attacks link the micro level insider characterization of psychological disposition with the above insider behaviour `UasI`. This is defined by the following rule `Insider a C` for the attacker `a`. The parameter `C` is a set of identities representing the members of an organisation. For the analysis of insider attacks that span over more than one company (see the Insider pattern "Ambitious Leader" in Section V-C) it is necessary to consider different organisations and their employees.

```
Insider a C ≡
tipping_point (astate a) ⟶ (∀ b ∈ C. UasI a b)
```

Although we characterize the above as a rule, it is not axiomatised; it is just a definition. We will use it as a local assumption (using the `assumes` feature of locales) in our case studies.

V. Applying the Isabelle/HOL Model to Case Studies

Finally, we illustrate the model and our methodology on case studies. We model the two insider threat patterns of Entitled Independent and Ambitious Leader in Isabelle/HOL showing how the three steps of social explanation are applied.

A. Insider Threat Patterns

The CERT Guide to Insider Threats [4] provides a 'breakdown of insider threats into three types of crimes: fraud, theft of Intellectual Property, and sabotage. [...] Insider IT sabotage crimes are those in which an insider uses IT to direct specific harm at an organisation or an individual. [...] Insider fraud cases are those in which an insider uses IT for the unauthorized modification, addition, or deletion of an organisation's data (not programs or systems) for personal gain, or theft of information which leads to an identity crime. [...] Insider theft of Intellectual Property [is] an insider's use of IT to steal intellectual property from the organisation.'

To show that our Isabelle/HOL model can serve as a general concept for the explanation of insider threats we use these patterns as benchmarks formalizing them in the framework introduced in the previous Section. Out of the three possible patterns of insider threat, we concentrate on insider theft of Intellectual Property. This pattern actually consists of two models [4]:

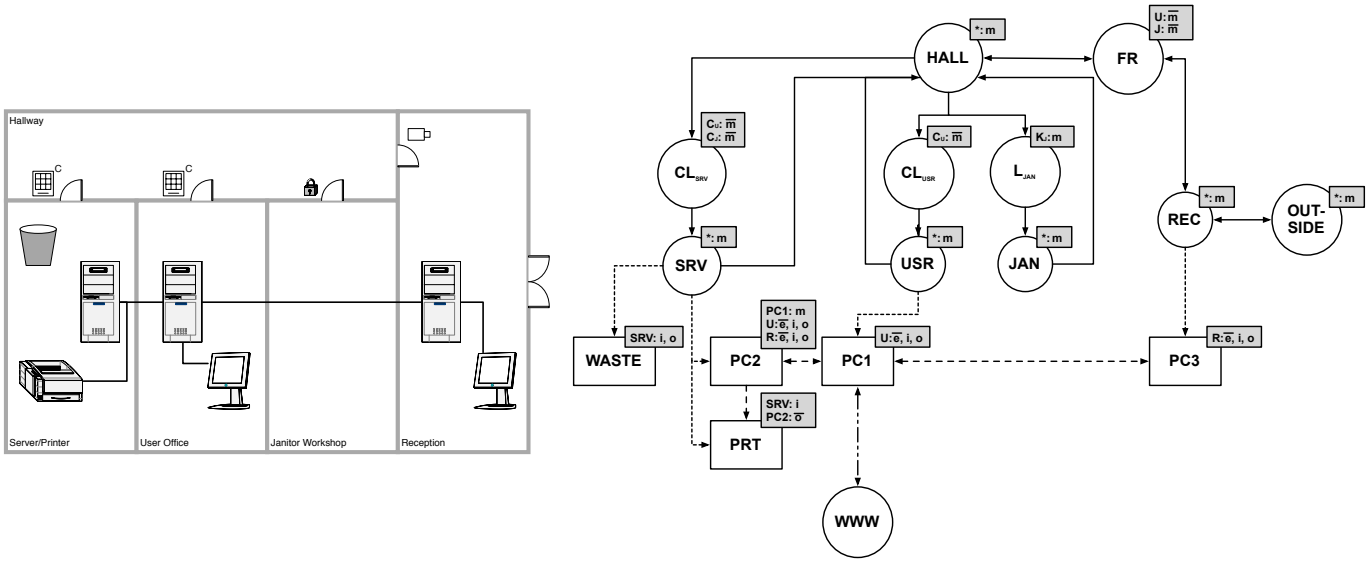

Fig. 2. A simple example system and its representation as a graph including actors, networks, locations, and policies in ExASyM [28]In our Isabelle/HOL framework, we represent these graphs algebraically.

- **Entitled Independent:** 'an insider acting primarily alone to steal information to take to a new job or to his own side business',
- **Ambitious Leader:** 'a leader of an insider crime who recruits insiders to steal information for some larger purpose.'

We do neither consider the patterns for fraud nor sabotage in this paper but we believe our framework to be capable of dealing with those equally well (see also Section VI for a discussion of that question). We do not follow the System Dynamics taxonomy given in the MERIT model but instead replace it by the similar taxonomy [24] formalized in Section IV-B since it subsumes the parts concerning the human disposition that are relevant for us.

B. Entitled Independent

The third step of social explanation leads the results of the actions of the individual actor at the micro level back to the macro level to explain the sociological phenomenon. In the insider threat patterns, this third step requires expressing the phenomenon: the insider breaks the organisation's policy. Therefore, we first need to define the global policy based on the local ones. Since the main effect is that of violating the global corporate policy, the effect to the macro-level is subsumed by the negated global policy: the attack of the insider has the effect that corporate data reaches the outside of the corporate network. Thus, the explanation consists of a proof in Isabelle/HOL that the insider can break the policy, i.e., the policy does not hold for him/her.

We give here a step by step description of the main analysis of the Entitled Independent case study. The full code is contained in the theory `EntitledIndependent.thy` available on the web at [23].

The case study uses our framework whose main module is the general theory for insiders in `Insider.thy`. Existing Isabelle/HOL theories can be imported to other theories. Here, we import `Insider`. To enable local definitions of a scenario for the Entitled Independent allowing the additional assumption of the necessary insiderness rules, we use the concept of locales and define locale `scenarioEI`.

```
theory EntitledIndependent
imports Insider
begin
locale scenarioEI =
```

We only model two identities, `Charly_comp` and `Charly_priv` representing actor Charly once as a member of the company and once as an outsider. We define the set of company actors as a local definition in the locale `scenarioEI`. We show here in a first instance the full Isabelle/HOL syntax but in all subsequent definitions we omit the `fixes` and `defines` keywords and also drop the types for clarity of the exposition. The full formalisation can be downloaded [23]. The double quotes `''s''` create a string in Isabelle/HOL.

```
fixes company_actors :: identity set
defines company_actors_def:
  company_actors ≡ {''Charly_comp''}
```

The graph representing the infrastructure of the Entitled Independent case study contains only the minimal structure.

```
company_locations ≡ {Location 1}
```

A global policy could be 'no corporate data must leave the corporate network' formalized in our HOL model using the enables statement (see previous Section) as follows.

```
global_policy I a ≡  a ∉ company_actors ⟶
    ¬(∃ t. t ∈ company_locations. enables I t a get)
```

Next, we have to provide the definition of the infrastructure. We first define the graph representing the organisation's locations and the positions of its actors. Locations are wrapped up with the datatype constructor `NL` and actors using the corresponding constructor `NA` to enable joining them in the datatype `node` and thus creating the following `node graph` as a set of pairs between locations or actors.

```
ex_graph ≡
    Graph {(NA (''Charly_comp''), NL (Location 1)),
           (NL (Location 2), NL (Location 1)),
           (NA (''Charly_priv''), NL (Location 2))}
```

Policies are attached to locations in the organisation's graph using a function that maps each location to the set of the policies valid in this location. The policies are again pairs. The first element of these pairs are credentials which are defined as predicates over actors, i.e., boolean valued functions describing, for example, whether an actor inhabits a role, or, whether an actor possesses something, like an identity or a key. The second elements are sets of actions that are authorised in this location for actors authenticated by the credentials.

```
local_policies ≡
  (λ x. if x = Location 1 then
     {(λ x. role (x, ''employee''), {get,put})}
       else (if x = Location 2 then
                  {((λ x. (ID x ''Charly_comp'') ∨
                           (ID x ''Charly_priv'')),
                  {get,put})}
             else {}))
```

For the final component of the infrastructure (the credentials in the `tspace`) we define the assignment of the credentials to the actors similarly as a predicate over actors that is true for actors that have the credentials.

```
ex_creds ≡ (λ x. if x = Actor ''Charly_comp'' then
                    role (x,''employee'')
                 else False)
```

Finally, we can put the graph, the local policies, and the credential assignment into an infrastructure.

```
EntInd_scenario ≡
 Infrastructure ex_graph local_policies ex_creds
```

Note, that all the above definitions have been implemented as local definitions using the locale keywords `fixes` and `defines`. Thus they are accessible whenever the locales `scenarioEI` is invoked but are not axioms that could endanger

consistency. We now also make use of the possibility of locales to define local assumptions. This is very suitable in this context since we want to emphasize that the following formulas are not general facts or axiomatic rules but are assumptions we make in order to explore the validity of the infrastructure's global policy. The first assumption provides that the precipitating event has occurred which leads to the second assumption that provides that Charly can act as an insider.

```
assumes Charly_precipitating_event:
  tipping_point (astate ''Charly_comp'')
assumes Insider_Charly :
  Insider ''Charly_comp'' {''Charly_priv''}
```

So far, we have specified the model. Based on these definitions and assumptions we can now state theorems about the security of the model and interactively prove them in our Isabelle/HOL framework. We can now first prove a sanity check on the model by validating the infrastructure for the "normal" case. For Charly as a company actor, everything is fine: the global policy does hold. The following is the statement of the Isabelle/HOL theorem `ex_inv` followed by the proof script of its interactive proof. The proof is achieved by locally unfolding the definitions of the scenario, e.g., `EntInd_scenario_def` and applying the simplifier.

```
lemma ex_inv:
 global_policy EntInd_scenario (''Charly_comp'')
by (simp add: EntInd_scenario_def global_policy_def
              company_actors_def)
```

However, since `Charly_comp` is at tipping point, he will ignore the global policy. This insider threat of the Entitled Independent can now be formalised as an invalidation of the global company policy for `''Charly_priv''`in the following "attack" theorem named `ex_inv1`.

```
theorem ex_inv1:
 ¬ global_policy EntInd_scenario ''Charly_priv''
```

The proof of this theorem consists of a few simple steps largely supported by automated tactics. As in the previous lemma, we first unfold the definitions leading to two subgoals in the interactive process of proving the theorem `ex_inv1` in Isabelle/HOL.

```
1. ''Charly_priv'' ∉ company_actors
2. ∃ t ∈ company_locations.
   enables
    (Infrastructure ex_graph local_policies ex_creds)
    t (Actor ''Charly_priv'') get
```

The first subgoal is solved by simplifying with the definition of `company_actors`. The difficult case is the second one since `''Charly_priv''` is not enabled to execute a `get` action on a company location. However, here the locale assumptions `Charly_precipitating_event` and `Charly_Insider` imply that

```
∀ b ∈ company_actors. UasI ''Charly_comp'' b
```

Hence, we can instantiate the universally quantified `b` with `''Charly_priv''` and derive that `Actor ''Charly_comp''` and `Actor ''Charly_priv''` are the same actor. Substituting now `Actor ''Charly_priv''` by `Actor ''Charly_comp''` in `2.` solves the second remaining subgoal and proves the goal. Summarizing, `Charly_priv` can get access to company data. This solves subgoal `2.` and thus finishes the proof of the theorem `ex_inv1` in our Isabelle/HOL framework for insider threats.

Results: The attack is proved above as an Isabelle/HOL theorem. Applying logical analysis, we thus exhibit that under the given assumptions the organisation's model is vulnerable to an insider. This overall procedure corresponds to the approach of invalidation of a global policy based on local policies for a given application scenario [5]. This earlier work on invalidation uses verification with modelchecking. The current approach using interactive theorem proving with Isabelle/HOL requires user interaction to exhibit the attack but there are advantages. First, we have no restriction on the complexity of the model; there is no risk of a state explosion as in modelchecking. We can explicitly express and reason about properties of all elements of our model. We already exploit this in the definition of the actors' state and the insider predicates in our insider theory that is then applied in the Entitled Independent analysis. Further extending this, we can use the higher expressiveness of HOL to elaborate the model to increase its resilience against insider attacks. A possible remedy, and thus a useful iteration in a practical application of our framework in designing or re-engineering a security architecture, would be to forbid sharing of Actor roles. In the following more complex insider threat pattern of the Ambitious Leader, this remedy is applied.

C. Ambitious Leader

The Ambitious Leader resembles the Entitled Independent. At least at the level of the taxonomy describing the mental disposition of the actors, i.e., the model of the micro level, we can reuse the same insider theory. The aspect that is more challenging in the Ambitious Leader pattern is the different setup of the infrastructure at the macro level. This pattern generalizes the Entitled Independent in that it is a combined attack between two organisations. The insider attack is only successful because the attacker can control two sub-insiders in two different companies. Here we have to extend the insider theory by a more refined insider predicate. The Ambitious Leader `Mallory` should be able to impersonate two sub-insiders `Charly` and `Carol` in two different organisations while these two cannot impersonate each other. However, with the previous insider predicate, `Insider Mallory {''Charly'', ''Carol''}` we would be able to prove that `Actor ''Charly'' = Actor ''Carol''` since the definition of `UasI` provides two equalities.

```
Actor ''Mallory'' = Actor ''Charly''
Actor ''Mallory'' = Actor ''Carol''
```

Since equality in HOL is an equivalence relation, i.e., reflexive, symmetric, and transitive, we immediately get that `Charly` and `Carol` can impersonate each other contradicting the assumptions of the Ambitious Leader scenario. Therefore, we

introduce here a less general insider predicate Insider'

```
Insider' P a C ≡
 (tipping_point (astate a) ⟶
  (∀ b∈ C. UasI' P a b ∧ inj_on Actor C))
```

This predicate demands that the function Actor must be injective on the set C which means that two Actors cannot share an identity if they are from the set C, i.e., the same company. In addition, we also use here a refined predicate UasI' that does not allow full equality of the Actors but only substitution in one direction in arbitrary contexts P. This variable P is a Higher Order function over the type actor.

```
UasI' P a b ≡ P (Actor b) ⟶ P (Actor a)
```

For illustration purposes, we keep the infrastructure model for the Ambitious Leader as small as possible while still expressing two organisations with the two sub-insiders Charly and Carol which are placed in two different locations corresponding to the two different organisations.

```
locale ambitious_leader =
  company_one_actors ≡ {''Charly''}
  company_two_actors ≡ {''Carol''}
  company_one_locations ≡ {Location 1}
  company_two_locations ≡ {Location 2}
```

The Ambitious Leader is represented by the third actor Mallory that is not a member of any of the two organisations. The global policy differs substantially in that it now reflects that actors that are not members of both organisations should not be enabled by the policies to get anything from the other company's locations.

```
global_policy I a ≡
 ¬(a ∈ company_one_actors ∨ a ∈ company_two_actors)
 ⟶  ¬((∃ t ∈ company_one_locations.
                  enables I t (Actor a) get)
       ∧(∃ t ∈ company_two_locations.
                  enables I t (Actor a) get))
```

The infrastructure graph contains the two organisations, their actors and also an "outside" location, Location 3 where the Ambitious Leader Mallory is positioned (see Figure 3).

```
ex_graph ≡
 Graph {(NA (''Charly''), NL (Location 1)),
        (NL (Location 3), NL (Location 1)),
        (NA (''Mallory''), NL (Location 3)),
        (NL (Location 3), NL (Location 2)),
        (NA (''Carol''), NL (Location 2))}
```

The local policies assigned to the companies' nodes implement that only employees of the corresponding organisations should have access.

```
 local_policies ≡ (λ x. if x ≡ Location 1 then
   {(λ x. role (x, ''employee_C_one''), {get,put})}
       else (if x = Location 2 then
   {((λ x. role(x, ''employee_C_two'')), {get,put})}
                          else {}))
```

The credentials assign the right roles to the employees Charly as being with the first company and Carol with the second.

```
  ex_creds ≡ (λ x. if x = Actor ''Charly'' then
```

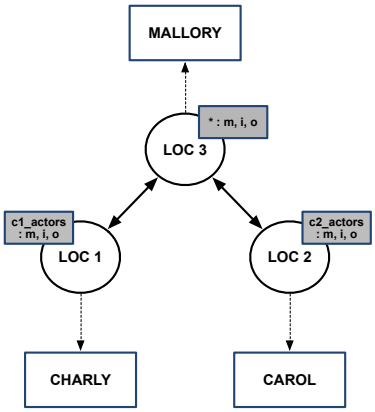

Fig. 3. Graphical representation of ambitious leader in ExASyM.

```
      role (x,''employee_C_one'')
      else
      (if x = Actor ''Carol'' then
        role (x,''employee_C_two'') else False))
```

As in the previous case study, we can then combine these elements into the infrastructure depicted in Figure 3.

```
amb_lead_scenario ≡
  Infrastructure ex_graph local_policies ex_creds
```

We can prove again as a sanity check that the global policy holds for each of the companies in isolation, i.e., the following two propositions are proved as theorems in the theory AmbitiousLeader.thy

```
global_policy amb_lead_scenario (''Charly'')
global_policy amb_lead_scenario (''Carol'')
```

Nevertheless, the ambitious leader Mallory can attack. We can prove the following "attack" theorem ex_inv2 in our Isabelle/HOL framework.

```
theorem ex_inv2:
¬ global_policy amb_lead_scenario (''Mallory'')
```

The locale assumptions that enable this proof are the following. Note, that we use here the refined insider characterisation Insider' introduced above.

```
assumes Mallory_precipitating_event:
  tipping_point (astate ''Mallory'')
assumes Insider_Mallory:
  Insider' (λ x. enables I t x a')
        ''Mallory'' {''Charly'', ''Carol''}
```

The proof of this final theorem ex_inv2 is slightly more complicated than in the previous case study of the Entitled Independent since we have to combine two insider attacks. Therefore, we have to show that Mallory can impersonate Charly in the first company and Carol in the second to break the global policy twice and use action get at the two locations.

Results: While the basic structure of the human disposition is the same for the Entitled Independent and the Ambitious Leader there are some decisive differences in the applications to the two case studies. Besides the different organisational scenarios that lead to different attacks, the impersonation

given by the extended predicate `UasI'` is more subtle. An important point that is nicely illustrated by this refinement of the impersonation predicate is that the explicit modeling of the actors and their identities enables a precise expression of what corresponds to authenticity: if the relationship between the identity and the actor that manifests this identity is an injective function then we implicitly formalize proof of identity. The expression of and reasoning about properties of functions, like injectivity of `Actor`, that are used in the model, is clearly a higher order feature not possible in first order logics or modal logics of model checkers. In general, reasoning at the macro level when using properties of the infrastructure while at the same time being able to reason at both macro and micro level enables also reasoning about the dispositions of actors in relation to the infrastructure context. This is necessary to formalize the macro-micro transitions of social explanation. For example, we can express in the insider theory the level of connectedness of actors in the social graph and its effects on the tipping point of an actor. It is important to see that this goes beyond what the propositional and modal logics of model checkers offer and thus shows the benefits of the HOL approach.

VI. Related Work

A. Own Previous Work

In own previous work [2], [5], we have used invalidation of security policies and subsequent modelchecking to discover possible insider attacks. In this earlier approach we already used organisational models similar to the ones presented here and expressed policies as propositional or temporal properties on these models. However, the organisational models had to be simplistic in nature to avoid the state explosion problem that is inherent in the modelchecking approach. On the other hand, we already noticed in these early experiments that a refinement of these simple models is often a very useful step to exhibit sufficient detail to discover an insider attack. For example, a date had to be added to a lottery ticket to make the backdating scam detectable [2]. However, it is exactly this kind of state variable that causes complex state spaces and impedes the modelchecking analysis. We thus already integrated Isabelle/HOL in these earlier experiments to verify refinement conditions between abstract and refined models. In the current work, we show that the verification of insider threats can be completely performed inside Isabelle/HOL. Compared to modelchecking, we need to perform proofs of policy violations interactively but the proofs are largely done by automated simplification in Isabelle/HOL. We extended the HOL model for insider threats [7] to cope with general insider threat patterns and validated this on the two general patterns Entitled Independent and Ambitious Leader.

B. Other Works

The CERT Guide to Insider threats [4] uses the System Dynamics modeling method. In this methodology abstract variables define a taxonomy of insider threat cases. Graphically, these variables are presented in square boxes. A solid arrow from a box containing variable a to one containing variable b indicates that an increase of a implies an increase of b. A dashed arrow represents the inverse relationship, i.e., that an increase of a corresponds to a decrease of b. In comparison to our way of modeling and analysing insider threats in HOL, this approach enables expression of a relationship between variables. However, this is an imprecise, i.e., not quantified dependency. Moreover, the modeling is constrained to the shallow expression of variables of a taxonomy and has no structure to model the various levels and structures we have in our HOL framework. Figure 4 shows a part of the pattern for IT sabotage, another one of the three main patterns of Insider Threat from the CERT guide [4]. The part shown concerns the modeling of the insider's disposition. It is very similar to the taxonomy we chose [24] as a basis for our Isabelle/HOL framework further supporting the generality of our approach.

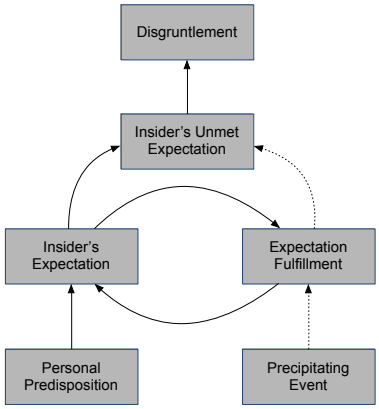

Fig. 4. The expectation escalation in the Systems Dynamics model for the IT sabotage insider threat pattern – another one of three [4, page 32].

The inductive approach to security protocol verification in Isabelle by Paulson [29], the designer of the Isabelle system, picked up on the hype generated by the earlier modelchecking approach to security by Lowe [30]. This approach is already sufficient to model the Lowe attack but it is not yet sufficiently expressive for insider threats. In comparison to modelchecking, the inductive approach is more laborious as it requires human interaction, but it is unrivaled in its expressiveness which allows proofs beyond the ones that are usually done in model checkers. The model chosen in the inductive approach can be seen as a micro-level representation of a global communication scenario. Social explanation is not explicitly addressed nor is any relation to sociology intended. The security protocol defines the 'normal' behaviour of communication partners and the Dolev-Yao model [31] characterizes the attacker's behaviour (sees all, can intercept, and send). The first step of situational logic (interpretation) is implicit in the inductive approach since the attacker has been already introduced. An explicit modeling of this first step needs to integrate a description of how a 'normal' principal turns into an attacker. This is what is additionally addressed in the social explanation approach by the transition from the macro to the micro level. It is arguable whether the proofs

of secrecy of keys in the inductive approach can be seen as the third step of micro to macro transition of the social explanation.

The application of HOL for human behavior modeling has been pioneered by Bella and Coles-Kemp in their formal consideration of *ceremonies* [32]. This concept expands a security protocol to include all those assumptions and other context information that was previously considered as 'out-of band'. Thus, like in our approach, a ceremony also considers the human factor as a central element. The main emphasis in ceremonies, and consequently also in Bella's and Coles-Kemp's work, is on incomplete or partial behaviour of humans, for example, incomplete comparison of values. Bella and Coles-Kemp propose a 'multiple-layer model' consisting of a stack of protocols. The lower part contains the technological protocol layers and the upper part the sociological layers. There is one unique interface (Layer III) where the socio-technological interaction is modeled and analyzed by state descriptions ('stances') in one direction: from the user to the computer interface. For insider attacks a more complete representation of actors, their internal state as well as their physical and organisational context is needed. Therefore, we model individual actors, their mental state, actions as well as locations that can be physical or logical entities.

Formal techniques for insider analysis have also been applied by Pieters, Dimkov, and Pavlovic [33]. They consider policy alignment to address different levels of abstraction of socio-technical systems. Policy alignment is in their view a refinement of policies to more concrete system representations. Policies are interpreted as first-order logical theories containing all sequences of actions (the behaviours) and expressing the policy as a 'distinguished' prefix-closed predicate in these theories. Refinement of consistent, i.e., policy-fulfilling specifications, is then readily provided by the completeness relation between first-order theories. Although the use of graphs as system representations and local policies attached to those graphs is used in the application example, contrary to our approach Pieters et al. do not use an explicit infrastructure model in their approach [33] but only an abstract formal notion of action sequences to represent systems.

VII. Conclusions

In this paper, we showed that Isabelle/HOL is suited to model insider threats based on the process of social explanation. We derived a characterization of an insider's capability to impersonate others from protocol verification. The use of Higher Order Logic permits the expression of the actor's mental disposition like motivation or psychological state. At the same time in a same theory, the infrastructure of an organisation including the physical network, logical policies and an abstract behaviour of actors in this network can be represented. Thus, human behaviour can be modeled for insider threats according to Weber's three steps of sociological explanation. Higher Order Logic allows formalisation of actors' properties for all three steps as we illustrated on the two general insider patterns of Entitled Independent and Ambitious Leader. This

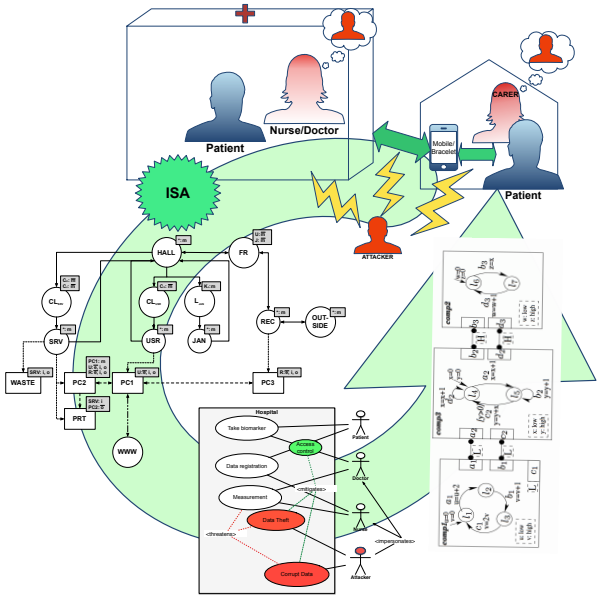

Fig. 5. Using multiple biosensors, each tailored to identify a specific bio marker, we propose a security architecture for cyber physical systems including humans that can be used in the home to provide objective data of the progression and possible causes of Alzheimer's disease. Step ISA shows where the Isabelle/HOL framework for social explanation is used to extract a secure infrastructure model and policies that can be fed into a development cycle for the architecture as use cases including insider attackers as actors.

illustration implicitly validates that insider attacks in general can be explained using social explanation. The model of the human disposition is very similar in one of the other two patterns (see Figure 4) strengthening this conjecture. There are many works on modeling human behaviour in psychology, sociology, and also human computer interaction. We have picked the approach of social explanation since it fits best our purpose of providing a logical framework for insider threat analysis. A detailed introduction to modeling and theory building in Higher Order Logic [7] compares it to the three step process of sociology. The process of construction of theories in HOL corresponds largely to the logic of explanation [19] underpinning social explanation (see Section III). We thus use HOL modeling here to analyse local policies within infrastructures in relation to global policies and their vulnerability to insiders threats.

The demonstration of social explanation contributes to the understanding of insider threats in complex infrastructures and also provides a framework for their modeling and analysis. This framework is an extension of the Isabelle/HOL proof assistant thus providing a dedicated tool for modeling concrete infrastructures of organisations and their security policies. Interactive proof with our Isabelle/HOL extension then allows proving violations of global policies by actions of malicious insiders. Detection of such violations can be used to improve the infrastructure and policies leading to an improved security architecture. Figure 5 shows how we envisage the integration of our framework for a privacy enhancing sensor network for the monitoring of dementia patients.

Interactive theorem proving in Isabelle/HOL shows yet again how expressive and thus powerful it is: human psychological dispositions, local and global policies, as well as physical and network aspects of organisation's infrastructures can be expressed in HOL. The price to pay for expressiveness is human interaction in proofs but at a high level of system development – like security architectures – human interaction seems natural. Beyond this application of the formalisation of social explanation to insider threats, we consider it worthwhile to explore our approach further also on the conceptual level and continue the elaboration of a general model of social explanation in Isabelle/HOL. The current work has provided a theory for the description of insiders at the macro and micro level as well as methods for the rigorous support of social explanation: the Insider predicate allows to link macro and micro level and the use of locales in Isabelle/HOL supports clear structuring of local insider assumptions for the verification of case studies. It is interesting to explore to what extent an independent theory of Weber's three steps can be formalized in Isabelle/HOL and meta-theoretic theorems can be proved. Such a theory would be beneficial to approach a systematic methodology for social explanation of cyber-humane systems even beyond insider threats.

REFERENCES

[1] Weber, M.: Die protestantische Ethik und der Geist des Kapitalismus. In: Max Weber, Gesammelte Aufsätze zur Religionssoziologie, Tübingen (1978) 7. edition, (first edition 1920).

[2] Kammüller, F., Probst, C.W.: Combining generated data models with formal invalidation for insider threat analysis. [35]

[3] Nipkow, T., Paulson, L.C., Wenzel, M.: Isabelle/HOL – A Proof Assistant for Higher-Order Logic. Volume 2283 of LNCS. Springer-Verlag (2002)

[4] Cappelli, D.M., Moore, A.P., Trzeciak, R.F.: The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). 1 edn. SEI Series in Software Engineering. Addison-Wesley Professional (February 2012)

[5] Kammüller, F., Probst, C.W.: Invalidating policies using structural information. [34]

[6] Glasser, J., Lindauer, B.: Bridging the gap: A pragmatic approach to generating insider threat data. [34]

[7] Boender, J., Ivanova, M.G., Kammüller, F., Primiero, G.: Modeling human behaviour with higher order logic: Insider threats. In: STAST'14, IEEE (2014) co-located with CSF'14 in the Vienna Summer of Logic.

[8] Burrows, M., Abadi, M., Needham, R.: A logic of authentication. ACM Transactions on Computer Systems **8** (1990) 18–36

[9] Needham, R.M., Schroeder, M.D.: Using encryption for authentication in large networks of computers. Communications of the ACM (21) (1978)

[10] Lowe, G.: An attack on the needham-schroeder public-key authentication protocol. Information Processing Letters **56**(3) (1995) 131–133

[11] Lowe, G.: Breaking and fixing the needham-schroeder public-key protocol using fdr. In: Tools and Algorithms for the Construction and Analysis of Systems, Springer-Verlag (1996) 147–166

[12] Popper, K.R.: Objektive Erkenntnis. Hoffmann und Campe (1993)

[13] Tarski, A.: Der wahrheitsbegriff in den formalizierten sprachen. Studia Philosophica **1** (1935) 261–405

[14] Tarski, A.: The semantic conception of truth: and the foundations of semantics. Philosophy and Phenomenological Research **4** (March 1944)

[15] Esser, H.: Soziologie – Allgemeine Grundlagen. Campus (1993)

[16] Weber, M.: Wirtschaft und Gesellschaft. Grundriss der verstehenden Soziologie. Tübingen (1972) 5. Auflage.

[17] Boudon, R.: Die Logik des gesellschaftlichen Handelns. Eine Einführung in die soziologische Denk- und Arbeitsweise. Darmstadt und Neuwied (1980)

[18] Schütz, A.: Begriffs- und theoriebildung in den sozialwissenschaften. In: Gesammelte Aufsätze, Band 1: Das Problem der sozialen Wirklichkeit. Springer Netherlands (1971) 55–76

[19] Hempel, C.G., Oppenheim, P.: Studies in the logic of explanation. Philosophy of Science **15** (April 1948) 135–175

[20] McClelland, D.C.: The achieving society. Van Nostrand, Princeton, NJ (1961)

[21] Kammüller, F., Wenzel, M., Paulson, L.C.: Locales - a sectioning concept for isabelle. In Bertot, Y., Dowek, G., Hirschowitz, A., Paulin, C., , Thery, L., eds.: Theorem Proving in Higher Order Logics, 12th International Conference, TPHOLs'99. Volume 1690 of LNCS., Springer (1999)

[22] Kammüller, F.: Modular reasoning in isabelle. In MacAllester, D., ed.: 17th International Conference on Automated Deduction, CADE-17. Volume 1831 of LNAI., Springer (2000)

[23] Kammüller, F.: Isabelle formalisation of an Insider threat framework with examples Entitled Independent and Ambitious Leader. https://www.dropbox.com/sh/rx8d09pf31cv8bd/AAALKtaP8HMX642fi040g4NLa?dl=0 (2015) Dropbox directory.

[24] Nurse, J.R.C., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R.T., Whitty, M.: Understanding Insider Threat: A Framework for Characterising Attacks. [35]

[25] Martinko, M.J., Grundlach, M.J., Douglas, S.C.: Toward an integrative theory of counterproductive workplace behaviour. International Journal of Selection and Assessment **10**(1–2) (2002) 36–50

[26] Marcu, B., Schuler, H.: Antecedents of counterproductive behaviour at work: a general perspective. Journal of Applied Psychology **89**(4) (2004) 647

[27] Probst, C.W., Hansen, R.R.: An extensible analysable system model. Information Security Technical Report **13** (2008) 235–246

[28] Probst, C.W., Hansen, R.R.: An extensible analysable system model. Information Security Technical Report **13**(4) (November 2008) 235–246

[29] Paulson, L.C.: The inductive approach to verifying cryptographic protocols. Journal of Computer Security **6**(1-2) (1998) 85–128

[30] Lowe, G.: Casper: A compiler for the analysis of security protocols. In: Computer Security Foundations Workshop (CSFW '97). (1997)

[31] Dolev, D., Yao, A.C.: On the security of public key protocols. In: 22nd Annual Symposium on Foundations of Computer Science, SFCS '81, IEEE (1981)

[32] Bella, G., Coles-Kemp, L.: Layered analysis of security ceremonies. In Gritzalis, D., Furnell, S., Theoharidou, M., eds.: SEC. Volume 376 of IFIP Advances in Information and Communication Technology., Springer (2012) 273–286

[33] Pieters, W., Dimkov, T., Pavlovic, D.: Security policy alignment: A formal approach. IEEE Systems Journal **7**(2) (2013) 275–287

[34] Proceedings of the second IEEE Workshop on Research in Insider Threats, WRIT'13. In: WRIT'13, IEEE (2013)

[35] Proceedings of the third IEEE Workshop on Research in Insider Threats, WRIT'14. In: WRIT'14, IEEE (2014)